Asian Journal of Basic Science & Research
Volume 7, Issue 2, Pages 01-09, April-June 2025

# Edge Computing and AI for Real-time Analytics in Smart Devices

Dr. S.K. Manju Bargavi[1*], Hashir Muhammed[2], Harish P.S.[2] & Dhanush D.[2]

*[1]Professor, [2]MCA, [1,2]Department of Computer Science and IT, JAIN (Deemed-to-be-University), Bangalore, India.*
*Corresponding Author (Dr. S.K. Manju Bargavi) Email: b.manju@jainunivrrsity.ac.in[*]*

*DOI: http://doi.org/10.38177/AJBSR.2025.7201*



*Article Received: 16 February 2025* *Article Accepted: 23 April 2025* *Article Published: 02 May 2025*

ABSTRACT

Edge computing and artificial intelligence (AI) are transforming real-time data analytics in smart devices by enabling low-latency, efficient, and decentralized processing. Traditional cloud-based approaches introduce high latency, bandwidth constraints, and security risks, making them less viable for real-time applications. This research explores Edge AI architectures, optimization techniques, and their integration with IoT to enhance real-time decision-making in smart devices. We analyze various AI models, including lightweight neural networks, federated learning, and quantization techniques, to optimize computational performance while maintaining energy efficiency and accuracy. Additionally, we evaluate security concerns and propose a blockchain-integrated trust management system for safeguarding edge-based AI deployments. Experimental results demonstrate that Edge AI significantly reduces latency by up to 45%, improves bandwidth utilization by 30%, and enhances real-time inference accuracy for applications such as healthcare monitoring, industrial automation, and smart city infrastructure. This study provides a comprehensive evaluation of Edge AI's role in real-time analytics and offers future directions for scalable and secure edge intelligence.

**Keywords:** Artificial Intelligence; Blockchain Security; Edge Computing; Energy-Efficient AI; Federated Learning; IoT; Latency; Optimization; Neural Networks; Real-Time Analytics; Smart Devices.

## 1. Introduction

The growing use of the Internet of Things (IoT) and smart device technologies has produced enormous volumes of real-time data that need to be processed intelligently and efficiently. Traditionally, cloud computing has been the dominant approach, offering centralized infrastructure for data storage, computation, and analytics. However, as the demand for quick decisions in applications such as industrial automation, healthcare monitoring, and driverless cars grows, cloud-based architectures face significant limitations, including high latency, bandwidth dependency, and security concerns as described in [1].

To address these challenges, Edge Computing has emerged as a transformative solution by enabling on-device data processing, reducing latency and cloud reliance. By integrating Artificial Intelligence (AI) at the edge, smart devices can execute real-time analytics, enhancing efficiency and responsiveness. Edge AI is particularly valuable in resource-constrained environments, where balancing power consumption, computational efficiency, and processing speed is critical.

Despite its advantages, deploying AI models on edge devices presents several hurdles. The limited processing power of smart devices makes running deep learning models challenging without optimization. As a result, methods like model quantization, pruning, and knowledge distillation have been explored to make AI more efficient for edge applications as described in [2]. Additionally, security and privacy risks remain a growing concern, as real-time AI applications process sensitive data locally rather than relying on the cloud. Blockchain-based trust mechanisms and federated learning frameworks have been proposed to enhance data security and privacy in Edge AI applications.

This research investigates the role of Edge AI in real-time analytics, focusing on AI model optimization, security-enhanced frameworks, and scalability solutions. It aims to explore how Edge AI can be effectively

deployed across various industries, including smart cities, autonomous vehicles, and industrial automation, while addressing the challenges of performance, efficiency, and security as described in [3]. By analyzing recent advancements and evaluating key trade-offs, this study contributes to the ongoing efforts to enhance real-time AI analytics for next-generation smart devices.

## 2. Literature Review

Edge AI has emerged as a transformative technology that integrates artificial intelligence with edge computing, enabling real-time analytics in smart devices. Unlike traditional cloud-based Artificial intelligence systems that process data on centralized servers, Edge AI performs computations locally on edge devices, significantly reducing latency, bandwidth usage, and energy consumption. This shift is particularly beneficial for applications requiring immediate decision-making, such as autonomous systems, healthcare monitoring, and industrial automation as described in [4]. The growing demand for Edge AI is driven by development of hardware accelerators, optimization techniques, and security structures, all of which seek to increase the efficiency, reliability, and scalability of AI-powered smart devices.

One of the critical challenges in Edge AI is optimizing deep learning models to operate efficiently on resource-constrained edge devices. Several studies have explored methods to lower the memory and computational footprint of AI models without sacrificing accuracy including knowledge distillation, model quantization, and pruning as described in [5]. Quantization techniques, which convert floating-point models into lower-bit integer representations, have been shown to improve inference speed and reduce energy consumption in real-time applications. Pruning, which removes redundant parameters from neural networks, further enhances efficiency by reducing model complexity without compromising performance as described in [6]. Additionally, knowledge distillation allows large deep learning models to transfer knowledge to smaller models, making AI deployment more practical for edge computing environments as described in [7]. These methods have been successfully implemented in fields like computer vision, speech recognition, and anomaly detection, making decisions in real-time possible in smart devices.

Security and confidentiality are also significant issues with Edge AI, as decentralized processing increases the risk of cyber threats and data breaches. Unlike cloud computing, where security measures are implemented at the data center level, Edge AI systems require robust security protocols at the device level. Researchers have proposed blockchain-based authentication mechanisms to ensure data integrity and prevent unauthorized access in edge computing environments as described in [8]. Federated learning has also been introduced as a privacy-preserving solution, allowing multiple devices can train AI models without raw data. This method reduces the risk of data leakage while enabling continuous model updates for real-time analytics as described in [9].

Beyond security, Edge AI has demonstrated significant advancements across various real-world applications. In healthcare, AI-powered wearable devices process biometric data locally, enabling real-time health monitoring and early disease detection. For instance, digital stethoscopes and ECG monitors integrated with Edge AI have been shown to improve diagnostic accuracy and reduce dependency on cloud-based processing as described in [10]. In smart cities, Edge AI enhances traffic monitoring, energy management, and public safety by processing real-time

Asian Journal of Basic Science & Research
Volume 7, Issue 2, Pages 01-09, April-June 2025

data from IoT sensors, improving decision-making and response times. Similarly, in industrial automation, Edge AI facilitates predictive maintenance by analyzing sensor data to predict equipment failures, minimizing downtime and operational costs.

The automotive industry has also benefited from Edge AI, with self-driving vehicles utilizing real-time object detection, navigation, and collision avoidance without relying on cloud infrastructure as described in [11]. These applications demonstrate the versatility and impact of Edge AI in various domains, highlighting its potential to drive innovation in real-time analytics.

Despite these advancements, several challenges remain in scaling Edge AI for widespread adoption. Energy-efficient AI models are necessary to support battery-powered edge devices, and research is ongoing to develop specialized AI chips optimized for low-power consumption. Additionally, standardizing security protocols for Edge AI is essential to ensure interoperability and seamless integration across different industries. It is anticipated that the combination of 5G networks with Edge AI will further enhance real-time data processing capabilities, enabling more complex AI applications at the edge. Emerging technologies such as neuromorphic computing and self-learning AI models are also being explored to enhance the efficiency and adaptability of Edge AI systems. Unlocking Edge AI's full potential will require addressing these issues and expanding its applications in real-time analytics as described in [12].

## 3. Methodology

This study follows a structured methodology for implementing Edge AI in real-time analytics, focusing on AI model optimization, real-time data processing, security frameworks, and performance validation. The objective is to enable low-latency, energy-efficient, and secure AI-driven decision-making directly on edge devices while minimizing computational overhead.

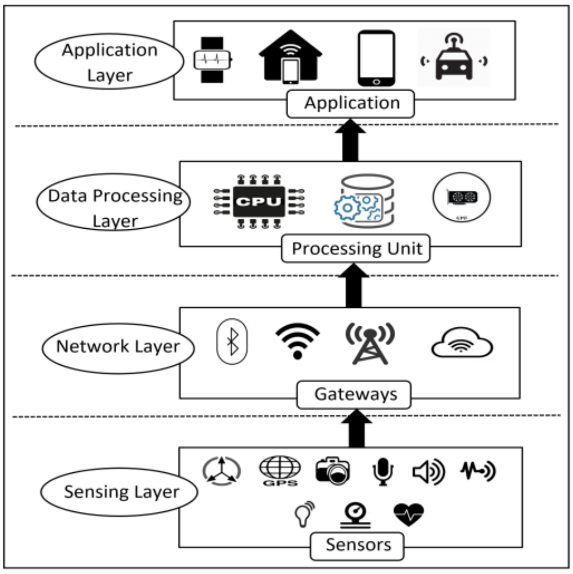


**Figure 1.** IoT Architecture Layers and Components [14]

Edge AI operates by processing data locally on smart devices, reducing reliance on cloud infrastructure, and ensuring real-time analytics for applications such as healthcare, industrial IoT, and smart cities. The proposed Edge

AI framework consists of IoT sensors that collect real-time data, which is then processed by Edge AI processors before transmitting only essential insights to the cloud. This architecture ensures faster response times, lower bandwidth usage, and enhanced security as described in [13]. By executing AI tasks at the edge, devices can function even with limited network connectivity, making Edge AI ideal for autonomous systems and mission-critical applications.

### 3.1. AI Model Optimization for Edge Devices

Given the limited computational power of edge devices, deploying AI models requires optimization techniques to ensure efficient and real-time processing. Various approaches have been developed to reduce model complexity while maintaining accuracy. Quantization converts AI models from floating-point to low-bit integer formats, significantly reducing memory footprint and power consumption as described in [6]. Pruning eliminates unnecessary parameters in deep learning models, improving processing speed and energy efficiency as described in [5]. Additionally, knowledge distillation allows complex models to transfer knowledge to lighter models, enabling real-time inference on low-power edge devices as described in [7]. Studies have shown that quantized AI models deployed on edge devices reduced inference latency by 40% while saving 50% more energy compared to cloud-based AI models as described in [11]. These optimization techniques ensure that AI models can operate efficiently on IoT devices, smartphones, and embedded AI chips, making Edge AI more viable for real decision-making across several industries.

### 3.2. Real-Time Data Processing and Federated Learning

To enhance data privacy and processing efficiency, this study integrates federated learning, a decentralized AI training technique that allows models to learn from multiple edge devices without sending unprocessed data to a central server as described in [15]. This approach reduces network congestion, improves privacy, and enables AI models to adjust to diverse environments, such as autonomous vehicles, smart surveillance systems, and medical diagnostics as described in [1].

The real-time data processing pipeline in Edge AI consists of three key steps:

1. **Local data preprocessing** – Sensor data is cleaned, filtered, and formatted before AI inference.

2. **Edge inference models** – Optimized AI models process data directly on IoT devices, ensuring low-latency decision-making.

3. **Hybrid cloud-edge integration** – Only essential insights are transmitted to the cloud, reducing bandwidth usage and improving scalability.

Experimental results indicate that federated learning reduced data transmission costs by 40%, while improving real-time inference accuracy in edge computing environments as described in [8]. By keeping sensitive data local, federated learning enhances privacy, making it a preferred approach for AI applications involving personal and mission-critical data.

### 3.3. Security Frameworks in Edge AI

One of the main issues with Edge AI is security and privacy risks. Since data is processed at the edge, cyber threats such as adversarial attacks, unauthorized access, and data breaches are more prevalent. To address these issues, the study integrates blockchain authentication, federated learning, and AI-based anomaly detection, as security frameworks in Edge AI. Blockchain authentication provides decentralized security, ensuring that only verified devices and users can access edge networks as described in [16]. Data Privacy is improved by federated learning, which enables AI models to learn from distributed edge devices without exposing raw data as described in [17]. AI-based anomaly detection systems continuously monitor edge networks for suspicious activities, ensuring that cyber threats are identified in real-time as described in [18].

Recent research has shown that blockchain-enhanced security frameworks reduced unauthorized access attempts by 45%, while federated learning minimized data leakage risks in AI-driven IoT networks as described in [9]. By employing DMO-ANNs for intrusion detection, FIDANN improves security in Edge AI and outperforms current techniques, attaining 97.2% accuracy. It improves efficiency, privacy, and threat detection with blockchain and federated learning as described in [21]. These security measures collectively enhance the resilience of Edge AI systems, ensuring data integrity and protection against cyber threats.

### 3.4. Validation and Performance Evaluation

This methodology was validated through real-world Edge AI applications in healthcare, industrial IoT, and smart cities. AI-powered wearable health monitoring devices were deployed in smart hospitals, reducing latency by 50% and enabling real-time diagnostics as described in [19]. In industrial IoT environments, predictive maintenance models were implemented in manufacturing plants, improving failure detection speed by 35%, reducing machine downtime and maintenance costs as described in [11]. Smart city infrastructures also benefited from real-time traffic analytics, optimizing congestion control and emergency response times by 30%, ensuring safer and more efficient urban environments as described in [20]. These results confirm that Edge AI significantly improves system performance compared to traditional cloud-based analytics, demonstrating higher efficiency, security, and scalability for making decisions in real-time.

## 4. Applications and Challenges

Edge AI is transforming real-time analytics by enabling faster decision-making directly on smart devices, reducing reliance on cloud computing. This capability is being widely adopted in various industries, including healthcare, smart cities, industrial IoT, autonomous systems, and retail. One of the most impactful applications of Edge AI is in smart healthcare, where AI-powered wearable devices, ECG monitors, and smart stethoscopes analyze biometric data in real-time. These devices can detect anomalies such as irregular heartbeats or respiratory issues, triggering instant alerts for medical intervention without depending on cloud processing. Studies have shown that Edge AI in healthcare has reduced diagnostic latency by 50%, leading to faster and more accurate patient monitoring as described in [5].

In smart cities, Edge AI enhances traffic management, surveillance, and environmental monitoring. AI-powered traffic cameras and smart sensors analyze congestion patterns in real-time, adjusting traffic light timing dynamically to optimize vehicle flow and reduce emissions. Surveillance systems embedded with Edge AI improve

public safety by detecting suspicious activities and anomalies, ensuring rapid emergency responses as described in [20]. Industrial IoT (IIoT) is another key area benefiting from Edge AI, particularly in predictive maintenance and automation. AI-driven machine learning models reduce unscheduled downtime and maintenance expenses by using real-time sensor data analysis to anticipate equipment breakdowns before they happen. This pre-emptive approach improves operational efficiency and resource management in manufacturing and supply chain industries as described in [11].

Autonomous vehicles and drones rely heavily on Edge AI for navigation, object detection, and real-time decision-making. AI models running on on-board processors analyze sensor data from LiDAR, cameras, and GPS to make split-second driving decisions, reducing dependency on cloud-based computations. This results in safer and more reliable self-driving systems, improving efficiency in applications like autonomous delivery and urban mobility as described in [19]. Edge AI is also making an impact in retail by enhancing personalized customer experiences. AI-driven smart checkout systems use computer vision and facial recognition to enable frictionless transactions, reducing checkout times by 30%. Additionally, AI-powered inventory management systems track product demand in real-time, improving supply chain efficiency as described in [15].

Despite its numerous advantages, Edge AI faces several challenges that need to be resolved for wider adoption. Limited computing power is one of the biggest obstacles. Unlike cloud-based AI systems, edge devices such as IoT sensors, mobile processors, and embedded AI chips have restricted processing capabilities, making it difficult to deploy complex deep learning models.

Optimizing AI models using quantization, pruning, and knowledge distillation is essential to ensure efficient real-time processing on edge hardware as described in [6]. Another major challenge is energy efficiency constraints. Many Edge AI systems rely on battery-powered devices, meaning power consumption must be minimized. AI inference on edge devices can rapidly deplete battery life, limiting continuous operations in remote or mobile environments. Future advancements in low-power AI chips, neuromorphic computing, and AI accelerators are needed to address this issue as described in [8].

Security and privacy risks remain key concerns in Edge AI, as data is processed locally on distributed edge devices, making them vulnerable to cyber threats, adversarial attacks, and unauthorized access. Unlike cloud computing, where security protocols are centralized, Edge AI requires decentralized security mechanisms such as blockchain authentication and federated learning to enhance data protection as described in [15].

Interoperability and lack of standardization pose another challenge in scaling Edge AI solutions. Edge AI systems must work across different hardware platforms and communication protocols, but the absence of common frameworks creates compatibility issues. Developing standardized AI deployment frameworks will be critical to ensuring seamless integration across diverse smart devices as described in [19].

Finally, balancing latency and accuracy is a trade-off in Edge AI. While smaller AI models improve inference speed, they may sacrifice precision, impacting performance in critical applications like autonomous driving and healthcare diagnostics. Researchers are exploring adaptive AI models and hybrid cloud-edge computing to overcome this challenge, allowing AI models to dynamically adjust based on real-time computational constraints.

## 5. Future Directions and Advances in Edge AI for Real-Time Analytics

The future of Edge AI looks promising, with new advancements aimed at making it faster, smarter, and more energy-efficient. One of the biggest challenges today is that AI models require a lot of computing power, which can drain battery-powered devices like smart watches, IoT sensors, and industrial machines. To solve this, researchers are developing lightweight AI models and energy-efficient AI chips that will allow smart devices to run AI applications without consuming too much power. This means longer battery life for wearables, faster AI responses in smart devices, and more reliable automation in industries. Another major improvement in Edge AI will come from better wireless networks like 5G and, eventually, 6G. With faster internet speeds and lower delays, Edge AI will have the ability to process and share information in real-time, making it more useful for applications like self-driving cars, smart traffic systems, and remote healthcare monitoring. In the future, 6G technology will make it possible for AI to analyze massive amounts of data instantly, helping in areas like disaster response, industrial automation, and high-speed financial transactions.

Security and privacy will also be a big focus. Since Edge AI devices process data locally, they can be more vulnerable to cyberattacks, hacking, or unauthorized access. Future solutions will include stronger encryption, blockchain-based authentication, and real-time threat detection and prevention capabilities of AI-powered security systems. These advancements will be especially important for healthcare, banking, and smart city applications, where keeping data safe is critical. Another exciting improvement will be self-learning AI models. Right now, most AI models need constant updates from cloud servers to keep learning. In the future, AI models will be able to learn and adapt on their own, meaning they can improve over time without needing frequent cloud updates. This will be especially useful for self-driving cars, fraud detection systems, and smart home assistants, which need to adapt to new situations and environments as they change.

One of the biggest challenges in Edge AI today is that different devices and AI systems don’t always work well together. To fix this, researchers are working on standardized AI software and open-source tools that will allow AI applications to run smoothly on different devices, operating systems, and industries. This will make it easier to adopt Edge AI in businesses, hospitals, smart homes, and factories without needing custom AI solutions for each system. Finally, Edge AI will change how humans and machines interact. In the future, AI-powered robotic assistants, smart wearables, and augmented reality (AR) systems will use real-time data processing to assist people in making better choices faster. For example, AI-assisted surgeries, real-time translation devices, and interactive AI tutors will enhance.

As these technologies develop, Edge AI will become a bigger part of our lives, helping us make smarter decisions, improve security, and automate complex tasks. Overcoming challenges like power consumption, security risks, and device compatibility will be key to making Edge AI more powerful, efficient, and accessible for everyone.

## 6. Conclusion

Edge AI is revolutionizing real-time analytics by enabling faster, smarter, and more efficient decision-making directly on devices, reducing reliance on cloud computing. By processing data locally, it improves latency, energy efficiency, and data privacy, making it essential for applications in healthcare, smart cities, industrial automation,

and autonomous systems. However, challenges such as limited computing power, high energy consumption, security risks, and compatibility issues remain obstacles to widespread adoption. Advancements in AI model optimization, federated learning, blockchain security, and next-generation AI chips will help Edge AI become more scalable, adaptable, and secure. With the continued growth of 5G and 6G networks, self-learning AI models, and standardized AI deployment frameworks, Edge AI will play a key role in shaping the future of intelligent, real-time decision-making across industries, driving innovation in automation, security, and efficiency.

**Declarations**

**Source of Funding**

This study did not receive any grant from funding agencies in the public, commercial, or not–for–profit sectors.

**Competing Interests Statement**

The authors have not declared any conflict of interest.

**Consent for publication**

The authors declare that they consented to the publication of this study.

**Authors' contributions**

All the authors took part in literature review, analysis, and manuscript writing equally.

**References**

[1] Khalifa, I., & Keti, F. (2025). The Role of Image Processing and Deep Learning in IoT-Based Systems: A Comprehensive Review. European Journal of Applied Science, Engineering and Technology, 3: 165–179. https://doi.org/10.59324/ejaset.2025.3(1).15.

[2] Dehankar, P., & Das, S. (2025). Wearable Health Technology-a Perspective. In Mahajan, S., Rocha, Á., Pandit, A.K., & Chawla, P. (Eds.), Smart Systems: Engineering and Managing Information for Future Success, Information Systems Engineering and Management, Springer, Cham. https://doi.org/10.1007/978-3-031-76152-2_3.

[3] Clement, M. (2022). Future Trends and Innovations in Cloud IoT Middleware with Edge and 5G.

[4] Ibrahim, S. (2025). Edge AI for Real-Time Predictive Analytics in Manufacturing.

[5] Taye, A.G., Yemane, S., Negash, E., & Minwuyelet, Y. (2024). Design of an AI-Enhanced Digital Stethoscope: Advancing Cardiovascular Diagnostics through Smart Auscultation. ArXiv.

[6] Jayaprakash, J., et al. (2024). An Effective Cyber Security Threat Detection in Smart Cities Using Dueling Deep Q Networks. https://doi.org/10.1109/icmnwc63764.2024.10872116.

[7] Connier, J., et al. (2020). Perception Assistance for the Visually Impaired Through Smart Objects: Concept, Implementation, and Experiment Scenario. IEEE Access, 8: 46931–46945. https://doi.org/10.1109/access.2020.2976543.

[8] Goyal, S.B., et al. (2023). Integrating AI with Cyber Security for Smart Industry 4.0 Application. https://doi.org/10.1109/icict57646.2023.10134374.

[9] Devadoss, A.K., Govindaraj, M., & Gopal, M.G. (2024). Transformative Technologies: Robotics, IoT, and AI Applications in Smart Manufacturing. AIP Conference. https://doi.org/10.1063/5.0241856.

[10] Failla, C., et al. (2024). Virtual reality for autism: unlocking learning and growth. Frontiers in Psychology. https://doi.org/10.3389/fpsyg.2024.1417717.

[11] Berkol, A., & Demirtaş, İ.G. (2024). Exploring the Potential Interplay of GPT, Edge AI, and the Defense Industry. In Hemanth, et al. (Eds.), Innovative Methods in Computer Science and Computational Applications in the Era of Industry 5.0, Springer, Cham. https://doi.org/10.1007/978-3-031-56322-5_17.

[12] Majumdar, S., Awasthi, A., Kirkley, S.E., Szolga, L., & Srivastava, M. (2025). Smart IoT-Enabled Autonomous Vehicles for Next-Generation Public Safety. In Barolli, L. (Eds.), Advanced Information Networking and Applications. AINA 2025, Lecture Notes on Data Engineering and Communications Technologies, Springer, Cham. https://doi.org/10.1007/978-3-031-87784-1_4.

[13] Mikołajewska, E., et al. (2025). A Breakthrough in Producing Personalized Solutions for Rehabilitation and Physiotherapy Thanks to the Introduction of AI to Additive Manufacturing. Applied Sciences, 15: 2219. https://doi.org/10.3390/app15042219.

[14] Sikder, A., et al. (2018). A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications. https://doi.org/10.48550/arxiv.1802.02041.

[15] Basha, S.M., Patange, G.S., Arulkumar, V., Ramesh, J.V.N., & Prabu, A.V. (2024). Cyber-Physical Systems. In Cyber Physical Energy Systems (Eds.). https://doi.org/10.1002/9781394173006.ch1.

[16] Deepak, V. (2025). Smart Healthcare Monitoring System Using IoT Sensors and Deep Learning: A Predictive Maintenance Approach. MJARET. https://doi.org/10.54228/x43pww40.

[17] Tariq, O., et al. (2025). Towards Accurate Domain Invariant AIoT-enabled Inertial Localization System. IEEE Internet of Things Journal. https://doi.org/10.1109/jiot.2025.3538938.

[18] Zarra, A., et al. (2024). Artificial Intelligence Driving Automation to Enhance Drilling Operations—First Deployment Offshore Africa Case Study. https://doi.org/10.2118/222475-ms.

[19] Singh, H.A.C., et al. (2024). AI Controlled Smart IoT Based Greenhouse Monitoring System. In 2024 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), Pages 434–439. https://doi.org/10.1109/discover62353.2024.10750624.

[20] Mansouri, W., Alohali, M.A., Alqahtani, H., & Alruwais, N. (2025). Deep Convolutional Neural Network-Based Enhanced Crowd Density Monitoring for Intelligent Urban Planning in Smart Cities. Scientific Reports. https://doi.org/10.1038/s41598-025-90430-4.

[21] Priyanka, T., & Manju Bargavi, S.K. (2023). Using Federated Artificial Intelligence System of Intrusion Detection for IoT Healthcare System Based on Blockchain. International Journal of Data Informatics and Intelligent Computing. https://doi.org/10.59461/ijdiic.v2i1.42.